

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/001437

<p><b>A. CLASSIFICATION OF SUBJECT MATTER</b>  Int.Cl<sup>7</sup> G09C1/00</p> <p>According to International Patent Classification (IPC) or to both national classification and IPC</p>														
<p><b>B. FIELDS SEARCHED</b></p> <p>Minimum documentation searched (classification system followed by classification symbols)  Int.Cl<sup>7</sup> G09C1/00</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005  Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  JSTPlus FILE</p>														
<p><b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b></p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>JP 2000-207483 A (Nippon Telegraph And Telephone Corp.), 28 July, 2000 (28.07.00), Par. Nos. [0041] to [0049]; Fig. 7 (Family: none)</td> <td>1</td> </tr> <tr> <td>Y A</td> <td>JP 2002-237810 A (NEC Corp.), 23 August, 2002 (23.08.02), Par. Nos. [0001] to [0009]; Fig. 10 &amp; US 2004/0114763 A1 &amp; EP 1361693 A1 &amp; WO 2002/065695 A1</td> <td>2-4 5</td> </tr> <tr> <td>Y A</td> <td>D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing 22, 14 May, 1990 (14.05.90), pages 503 to 513</td> <td>2-4 5-10</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	JP 2000-207483 A (Nippon Telegraph And Telephone Corp.), 28 July, 2000 (28.07.00), Par. Nos. [0041] to [0049]; Fig. 7 (Family: none)	1	Y A	JP 2002-237810 A (NEC Corp.), 23 August, 2002 (23.08.02), Par. Nos. [0001] to [0009]; Fig. 10 & US 2004/0114763 A1 & EP 1361693 A1 & WO 2002/065695 A1	2-4 5	Y A	D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing 22, 14 May, 1990 (14.05.90), pages 503 to 513	2-4 5-10
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.												
X	JP 2000-207483 A (Nippon Telegraph And Telephone Corp.), 28 July, 2000 (28.07.00), Par. Nos. [0041] to [0049]; Fig. 7 (Family: none)	1												
Y A	JP 2002-237810 A (NEC Corp.), 23 August, 2002 (23.08.02), Par. Nos. [0001] to [0009]; Fig. 10 & US 2004/0114763 A1 & EP 1361693 A1 & WO 2002/065695 A1	2-4 5												
Y A	D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing 22, 14 May, 1990 (14.05.90), pages 503 to 513	2-4 5-10												
<p><input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.</p>														
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>														
<p>Date of the actual completion of the international search 24 May, 2005 (24.05.05)</p>		<p>Date of mailing of the international search report 07 June, 2005 (07.06.05)</p>												
<p>Name and mailing address of the ISA/ Japanese Patent Office</p>		<p>Authorized officer</p>												
<p>Facsimile No.</p>		<p>Telephone No.</p>												

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/001437

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Y. Ishai and E. Kushilevitz, "Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation", IEEE Symposium on Foundations of Computer Science 2000, 22 January, 2001 (22.01.01), pages 294 to 304	6-10

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/001437

## Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The matter common to the inventions of claims 1-10 relates to a technique for calculating a given function by successively performing calculation by one computer after another which are linked to a device (hereinafter, referred to "technique X"). However, the search has revealed that the technique X is not novel since it is disclosed in document JP 2000-207483 A (NEC Corp.), 28 July, 2000 (28.07.00), Par. No. [0041] to [0049], Fig. 7. As a result, the technique X makes no contribution over the prior art and the common matter (technique X) cannot be a special technical feature within the meaning of PCT Rule 13.2, second sentence.

(Continued to extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

### Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/001437

Continuation of Box No.III of continuation of first sheet(2)

Accordingly, there exists no matter common to all the inventions of claims 1-10. The inventions of claims 1-10 are divided into three groups: the invention of claim 1, the inventions of claims 2-5, and the inventions of claims 6-10. Since between these groups of inventions, there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence, no technical relationship within the meaning of PCT Rule 13 between the different inventions can be seen. Consequently, it is obvious that the inventions of claims 1-10 do not satisfy the requirement of unity of invention.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

IntCl<sup>7</sup> G09C1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

IntCl<sup>7</sup> G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JSTPlusファイル

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-207483 A (日本電信電話株式会社) 2000.07.28, 段落【0041】 — 【0049】, 図7 (ファミリーなし)	1
Y A	JP 2002-237810 A (日本電気株式会社) 2002.08.23, 段落【0001】 — 【0009】, 図10 & US 2004/0114763 A1 & EP 1361693 A1 & WO 2002/065695 A1	2-4 5
Y A	D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing	2-4 5-10

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

24.05.2005

国際調査報告の発送日 07.6.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5S

3574

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	22, 1990.05.14, p.503-513  Y. Ishai and E. Kushilevitz, "Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation", IEEE Symposium on Foundations of Computer Science 2000, 2001.01.22, p.294-304	6-10

## 第II欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第III欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求の範囲1-10に係る発明の共通の事項は、機器を構成する複数の計算装置を連鎖させ、順に計算を行ってゆくことにより、与えられた関数の値を計算する技術（以下「技術X」という。）である。しかしながら、調査の結果、技術Xは、文献JP 2000-207483 A（日本電信電話株式会社）2000.07.28、段落【0041】-【0049】、図7に開示されているから、新規でないことが明らかとなった。結果として、技術Xは先行技術の域を出ないから、PCT規則13.2の第2文の意味において、この共通事項（技術X）は特別な技術的特徴ではない。それ故、請求の範囲1-10に係る発明全てに共通の事項はなく、請求の範囲1-10は、請求の範囲1に係る発明、請求の範囲2-5に係る発明、及び、請求の範囲6-10に係る発明の3群の発明に分けられるものと認められる。これら3群の発明は、PCT規則13.2の第2文の意味において特別な技術的特徴と考えられる他の共通の事項は存在しないので、それらの相違する発明の間にPCT規則13の意味における技術的な関連を見いだすことはできない。よって、請求の範囲1-10に係る発明は発明の単一性の要件を満たしていないことが明らかである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。  
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。